In the claims:

1. (previously presented) A method of securing packet data transferred between a first and second member of a private network coupled to client edge devices over a backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

encapsulating a private address of a packet from the first member with a group header including a public address associated with the first member and a group address to generate a tunneled packet;

transforming, at a client edge device, the tunneled packet by first applying a group security association associated with the private network to the tunneled packet to provide a secure tunneled packet and then adding a header field to the secure tunneled packet, the added header field including a gateway address associated with the first member of the private network and a destination address of the second member of the private network to provide a client transformed packet;

forwarding the client transformed packet to a provider edge device; and

replacing, at the provider edge device, a destination field of the packet with a group identifier associated with the private network for routing the packet across the backbone .

2. (cancelled)

3. (cancelled)

4. (cancelled)

5. (cancelled).

6. (original) The method according to claim 1, wherein the group security association is associated with each member of the private network.

7. (original) The method according to claim 1, further comprising the steps of:

each member of the private network registering with a global security server;

the global security server forwarding the group security association to each member of the private network.

8. (original) The method according to claim 7 including the step of the global security server periodically forwarding a new group security association to each member of the private network.

9. (previously presented) A method of securing packet data transferred between a first and second member of a private network over a backbone, the first and second member of the private network being coupled to respective client edge devices and the backbone comprising a plurality of provider devices including provider edge devices, the backbone operating according to a routing protocol, the method comprising the steps of:

determining, responsive to a gateway address of a packet, whether a packet received from a client edge device at a provider edge device of the backbone has been transformed to secure packet data transferred across the backbone;

modifying at least one field of the packet to replace a destination address of the packet with a group identifier associated with the private network responsive to a determination that the gateway address of the packet indicates that the packet is a member of the private network.

10. (cancelled)

11. (previously presented) A system for transforming packets for forwarding between a plurality of members coupled to client edge devices of a private network over a backbone comprised of a plurality of provider devices including provider edge devices in a scalable private network, wherein the backbone operates according to a protocol, the apparatus comprising:

a key table, the key table including a security association for each private network that the node is a member;

a client edge device including:

a tunneling mechanism for encapsulating packets that are to be transferred to the backbone in a public address including a gateway address and a group address to provide a tunneled packet; and

transform logic operable to apply a security association to the tunneled packet and to append a header to the tunneled packet, the header including a gateway address and a destination address to provide a transformed packet for transmission by the client edge device to the backbone;

a provider edge device coupled to the client edge device, the provider edge device comprising a virtual route forwarding table for storing group identifiers associated with destination addresses and means, responsive to the gateway address of the header, for selectively updating the destination field of the packet with a group identifier for routing the packet across the backbone.

12. (cancelled)

13. (cancelled)

14. (cancelled)

15. (cancelled)